Algebra Lineare e Geometria Analitica

Francesco Capocasa Costantino Medori

Nulla dies sine linea

Indice

Capitolo 1

ELEMENTI DI TEORIA DEGLI INSIEMI

1.1 Insiemi e classi

Con la parola *classe* si intende una collezione, un aggregato di oggetti di qualsiasi tipo. Gli oggetti che costituiscono una classe vengono detti *elementi*.

I concetti di classe, elemento, appartenenza sono assunti come primitivi, cioè di essi non viene data una definizione rigorosa (questa richiederebbe a sua volta concetti già rigorosamente definiti e così via), ma viene soltanto detto che tipo di idea farsene.

Una classe è ben individuata quando, in linea di principio, è possibile stabilire, dato un elemento a, se a appartenga alla classe in questione oppure non appartenga. Possiamo pensare a molti modi per realizzare questo: ad esempio, compilando l'elenco di tutti gli elementi che appartengono alla classe data, oppure indicando una proprietà che caratterizzi la classe, cioè che sia verificata da tutti e soli gli elementi di tale classe.

Il fatto che un elemento x appartenga alla classe A si indica scrivendo $x \in A$. Il fatto che x non appartenga ad A si scrive $x \notin A$.

Le classi che sono elementi di altre classi sono dette *insiemi* e sono quelle di maggior rilievo in matematica. Questa distinzione tra insiemi e classi proprie, che non possono essere considerate elementi di altre classi, serve ad evitare le spiacevoli contraddizioni che sorgono quando si vorrebbero considerare insiemi troppo grandi, come ad esempio l'insieme di tutti gli insiemi.

Valga per tutti il seguente esempio di *paradosso di Russell*. Sia I l'insieme di tutti gli insiemi X tali che $X \notin X$, cioè che non sono elementi di se stessi. Ad esempio, l'insieme $\mathbb{Z}$ dei numeri interi, non essendo un numero intero, appartiene a I. Domanda: $I \in I$? Risposta: se $I \notin I$, allora, per come è definito I, non essendo elemento di se stesso, $I \in I$. Se supponiamo $I \in I$, allora non soddisfa la proprietà che caratterizza I, cioè il non essere elementi di se stessi, e quindi $I \notin I$. Paradosso. Fortunatamente non ci imbatteremo più in questioni simili.

Un insieme S si dirà *sottoinsieme* dell'insieme A, o che S è incluso in A, se ogni elemento di S è anche elemento di A. Questo fatto si scrive $S \subseteq A$ o anche $S \subset A$.

Due insiemi sono uguali se e solo se hanno gli stessi elementi. Risulta allora chiaro che:

$$A = B \iff A \subseteq B \text{ e } B \subseteq A\,.$$

Supporremo l'esistenza di un insieme privo di elementi detto *insieme vuoto*, e indicato con il simbolo $\emptyset$, caratterizzato dalla proprietà: $a \notin \emptyset$ per ogni elemento a. L'insieme vuoto è incluso in ogni insieme e pertanto è unico.

Definizione 1.1.1 *Dati due insiemi A e B chiamiamo* unione *di A e B, in simboli, $A \cup B$, l'insieme degli elementi x tali che $x \in A$ oppure $x \in B$.*

L'unione di due insiemi è quell'insieme che ha come elementi tutti gli elementi di A e anche tutti gli elementi di B, ma non altri.

L'unione di due insiemi gode delle seguenti proprietà:

1) $A \cup (B \cup C) = (A \cup B) \cup C$ (associativa),
2) $A \cup B = B \cup A$ (commutativa),
3) $A \cup \emptyset = A\,.$

Definizione 1.1.2 *Dati due insiemi A e B chiamiamo* intersezione *tra A e B, in simboli, $A \cap B$, l'insieme degli elementi x tali che $x \in A$ e anche $x \in B$.*

L'intersezione di due insiemi è quell'insieme che ha come elementi tutti gli elementi di A che sono anche nel contempo elementi di B. L'intersezione gode delle seguenti proprietà:

1) $A \cap (B \cap C) = (A \cap B) \cap C$ (associativa),
2) $A \cap B = B \cap A$ (commutativa),
3) $A \cap \emptyset = \emptyset\,.$

Valgono inoltre le seguenti proprietà distributive:
4) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
5) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Definizione 1.1.3 *Chiameremo* differenza *tra A e B, e scriveremo $A - B$, oppure $A \setminus B$, l'insieme degli elementi x tali che $x \in A$ e $x \notin B$.*

È facile verificare che $(A - B) \cap (B - A) = \emptyset$. Nel caso in cui sia $B \subseteq A$, l'insieme $A - B$ si dice *complementare* di B rispetto ad A e si scrive $\mathcal{C}_A(B)$.
Valgono le *formule di de Morgan*:
1) $\mathcal{C}_U(A \cap B) = \mathcal{C}_U(A) \cup \mathcal{C}_U(B)$,
2) $\mathcal{C}_U(A \cup B) = \mathcal{C}_U(A) \cap \mathcal{C}_U(B)$.
dove A e B sono sottoinsiemi dello stesso insieme U.

Definizione 1.1.4 *Si dice* coppia *un insieme di due elementi. Una coppia in cui sia stato fissato un ordine secondo cui vi è un primo ed un secondo elemento, viene detta* coppia ordinata.

Se $\{a, b\}$ è una coppia, con (a, b) si indica la coppia ordinata avente a come primo elemento . Ovviamente in generale $(a, b) \neq (b, a)$.

Definizione 1.1.5 *Dati due insiemi A e B si dice* prodotto cartesiano *di A e B l'insieme di tutte le coppie ordinate (a, b) tali che il primo elemento della coppia appartenga ad A e il secondo elemento appartenga a B. Il prodotto cartesiano di A e B si indica con $A \times B$:*

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\} .$$

Osserviamo che $A \times B$ è in generale diverso da $B \times A$.
Di solito, i prodotti cartesiani sono degli insiemi ambiente, di cui ha particolare importanza studiare alcuni rilevanti sottoinsiemi.

Esempio 1.1.6 *1) Consideriamo gli insiemi $A = \{a, b, c, d, e, f, g, h, i, l\}$ e $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Se fissiamo un sottoinsieme $F \subseteq A \times B$ con particolari caratteristiche, e lo chiamiamo flotta, la determinazione di F da parte di un'altra persona si chiama battaglia navale.*
2) Sia l'insieme dei numeri reali. Il prodotto $\mathbb{R} \times \mathbb{R}$, che viene indicato anche con $\mathbb{R}^2$, è il cosiddetto piano cartesiano ed è l'ambiente di cui si studiano dei particolari sottoinsiemi detti rette, cerchi, coniche ecc.

1.2 Relazioni

Come visto nel caso di $\mathbb{R}$, anche per un qualsiasi insieme A possiamo considerare il prodotto $A \times A$ di due copie dello stesso insieme. Questo ci permette di formalizzare il concetto di *relazione* che risulta molto utile e che nel linguaggio comune necessita di difficoltose formulazioni.

Definizione 1.2.1 *Una* relazione binaria *su un insieme A è un sottoinsieme $\mathcal{R} \subseteq A \times A$. Diremo che due elementi a e b di A sono in relazione tra loro rispetto a $\mathcal{R}$ se $(a, b) \subseteq \mathcal{R}$.*

Esempio 1.2.2 *Sia $A = \{1\,,2\,,3\,,4\,,5\,,6\}$. La relazione "è divisore di" è individuata da $\mathcal{R} \subseteq A \times A$, dove*

$$\mathcal{R} = \{(1,1)\,,(1,2)\,,(1,3)\,,(1,4)\,,(1,5)\,,(1,6)\,,(2,2)\,,\\ (2,4)\,,(2,6)\,,(3,3)\,,(3,6)\,,(4,4)\,,(5,5)\,,(6,6)\}\,.$$

Continueremo per comodità in seguito ad utilizzare le locuzioni verbali per definire le relazioni su insiemi, salvo i casi in cui questo non sia o particolarmente scomodo (vi sono relazioni poco ragionevoli e giustificabili col senso comune) o dia luogo a qualche ambiguità.

Vogliamo ora indicare alcune proprietà di cui godono alcune relazioni binarie che rivestono particolare interesse in matematica.

Definizione 1.2.3 *Proprietà:*
1) riflessiva: $(a, a) \in \mathcal{R}$ *per ogni* $a \in A$,
2) simmetrica: $(a, b) \in \mathcal{R} \Rightarrow (b, a) \in \mathcal{R}$,
3) transitiva: $(a, b) \in \mathcal{R}$ *e* $(b, c) \in \mathcal{R} \Rightarrow (a, c) \in \mathcal{R}$,
4) antisimmetrica: $(a, b) \in \mathcal{R}$ *e* $(b, a) \in \mathcal{R} \Rightarrow a = b$.

Esempio 1.2.4
1. *Tra i numeri interi, la relazione "essere multiplo di" gode delle proprietà sopra 1), 3), 4), ma non della 2).*
2. *Tra le persone, la relazione "essere padre di" non gode di nessuna delle quattro proprietà.*
3. *La relazione "essere fratello/sorella di" gode della 2), 3) e, secondo qualche accezione, anche della 1).*
4. *La relazione "abitare nella stessa città di" gode delle 1), 2) e 3).*

5. *La relazione "abitare nel raggio di 10 Km da" gode della 1) e della 2), ma non della 3).*

6. *La relazione tra rette del piano "essere parallela a" gode delle 1), 2) e 3).*

7. *La relazione tra rette "essere perpendicolare a" gode solo della 2).*

8. *Tra i numeri interi, la relazione "la differenza è un multiplo di 5" (cioè: se $a, b \in \mathbb{Z}$, $(a, b) \in \mathcal{R} \Leftrightarrow (a-b)$ è un multiplo di 5) gode delle proprietà 1), 2) e 3).*

Definizione 1.2.5 *Una relazione binaria sull'insieme A viene detta* relazione di equivalenza *se gode delle proprietà riflessiva, simmetrica e transitiva.*

Sono relazioni di equivalenza quelle degli esempi 4, 6 e 8.

Per comodità, se a e b sono in relazione secondo la relazione di equivalenza $\mathcal{R}$ fissata, scriveremo $a \sim b$ in luogo di $(a, b) \in \mathcal{R}$ e leggeremo a è equivalente a b.

Definizione 1.2.6 *Sia A un insieme su cui è definita una relazione di equivalenza. Se $a \in A$, il sottoinsieme $C[a]$ di tutti gli elementi di A equivalenti ad a*

$$C[a] = \{x \in A \,|\, x \sim a\}\,,$$

si dice classe di equivalenza *di a. Esso si indica anche con $[a]$.*

Proposizione 1.2.7 *Sia A un insieme su cui è definita una relazione di equivalenza e siano a e b due elementi di A. Allora:*

$$C[a] \cap C[b] = \emptyset \text{ oppure } C[a] = C[b]\,.$$

Dim. Basterà dimostrare che se esiste $d \in C[a] \cap C[b]$ (ossia $C[a] \cap C[b] \neq \emptyset$), allora necessariamente $C[a] = C[b]$. Supponiamo che esista un tale d. Se $x \in C[a]$, $x \sim a$. Ma poiché $a \sim d$ e $d \sim b$, per la proprietà transitiva, $a \sim b$ e, sempre per lo stesso motivo, $x \sim b$, ossia $x \in C[b]$. Questo prova che $C[a] \subseteq C[b]$. Ripetendo lo stesso ragionamento partendo da $y \in C[b]$, si arriva a concludere che $C[b] \subseteq C[a]$ e quindi la tesi. □

L'insieme di tutte le classi di equivalenza di un insieme rispetto alla relazione di equivalenza viene detto *insieme quoziente*. Ad esempio, è interessante osservare che l'insieme quoziente della relazione dell'esempio 8) è

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\} ,$$

dove $[n]$ è la classe a cui appartiene n. Con $\mathbb{Z}_p$ si indica l'insieme quoziente rispetto alla relazione ottenuta sostituendo nella 8) il numero p al numero 5; esso si dice insieme degli *interi modulo p*.

Definizione 1.2.8 *Una famiglia di sottoinsiemi di un insieme A costituisce una* partizione *di A se l'unione di tutti gli insiemi della famiglia coincide con A mentre l'intersezione a due a due di tali insiemi è vuota.*

Proposizione 1.2.9 *Le classi di equivalenza costituiscono una partizione dell'insieme su cui è definita una relazione di equivalenza.*

Dim. La Proposizione 1.2.9 ci dice che classi di equivalenza distinte sono disgiunte (cioè con intersezione vuota). Resta da far vedere che l'unione delle classi dà tutto A. Per ogni $a \in A$, $a \sim a$ e dunque $a \in C[a]$. □

Per esercizio, dimostrare che, viceversa, data una partizione di un insieme A, essa determina su A una relazione di equivalenza così definita: $a \sim b$ se e solo se a e b appartengono allo stesso sottoinsieme della partizione. Osserviamo che, data una partizione di A, ogni elemento di A appartiene ad uno ed un solo sottoinsieme della partizione.

Definizione 1.2.10 *Una relazione $\mathcal{R}$ su A si dice* relazione d'ordine parziale *se gode delle proprietà riflessiva, transitiva e antisimmetrica.*

Si dice parziale perché esistono elementi non confrontabili, cioè: $(a, b) \notin \mathcal{R} \not\Rightarrow (b, a) \in \mathcal{R}$.

Esempio 1.2.11 *Sia $\mathcal{P}(A)$ l'insieme di tutti i sottoinsiemi di A, detto insieme delle parti di A. La relazione di inclusione è una relazione d'ordine parziale su $\mathcal{P}(A)$. Anche l'esempio 1.2.4. 1) è una relazione d'ordine parziale.*

Definizione 1.2.12 *Una relazione d'ordine parziale $\mathcal{R}$ viene detta* relazione d'ordine totale *se gode anche della seguente proprietà, detta* proprietà dicotomica*:*

$$\forall a, b \in A\,, (a, b) \notin \mathcal{R} \Longrightarrow (b, a) \in \mathcal{R}\,.$$

È una relazione d'ordine totale sull'insieme dei numeri reali la relazione "è maggiore o uguale a".

Esercizio 1.2.13 *Determinare tutte le relazioni d'ordine, sia parziale sia totale che possono essere date sull'insieme* $\{1, 2, 3\}$.

1.3 Applicazioni

Introduciamo ora il concetto di applicazione tra insiemi, o di funzione, termini che useremo come sinonimi, ma che è possibile trovare in giro con significati leggermente diversi.

Definizione 1.3.1 *Siano A e B insiemi non vuoti. Una* applicazione *dall'insieme A nell'insieme B è un sottoinsieme G di $A \times B$ tale che:*

$$\textit{per ogni } a \in A \textit{ esiste un } \text{unico } b \in B \textit{ tale che } (a, b) \in G.$$

Parlando intuitivamente, però, una applicazione è una regola, un criterio, un qualsiasi metodo che permetta di associare in un modo unico, senza ambiguità, indipendentemente cioè da chi esegua una tale operazione, a ogni elemento a di A uno ed un solo elemento b di B. Si può tranquillamente continuare a pensare ad una applicazione come ad una regola e considerare l'insieme G della definizione come il grafico della funzione. D'altra parte, formalizzare il concetto di regola è alquanto difficile ed il metodo più diretto per farlo è proprio questo: per sapere qual è l'elemento di $b \in B$ associato all'elemento $a \in A$, basta individuare l'unica coppia ordinata di G che abbia a come primo elemento e considerare il secondo elemento b di tale coppia.

Un po' di notazioni. Una applicazione f tra A e B si indica con

$$f : A \to B\,.$$

Se $b \in B$ è l'elemento associato all'elemento $a \in A$ dalla funzione f, si scrive

$$b = f(a)\,.$$

L'elemento $b = f(a)$ viene detto *immagine* di a.
Se $S \subseteq A$, $f(S) = \{b \in B \mid b = f(s) \text{ per qualche } s \in S\}$.
Se $C \subseteq B$, $f^{-1}(C) = \{a \in A \mid f(a) \in C\}$.

Come utile esercizio per impratichirsi con queste definizioni-notazioni, si verifichi che:

1. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$,
2. $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$,
3. $f(S \cup T) = f(S) \cup f(T)$,
4. $f(S \cap T) \subseteq f(S) \cap f(T)$, (ma in generale non vale l'uguaglianza),

dove $f : A \to B$, $X, Y \subseteq B$ e $S, T \subseteq A$.

Esempio 1.3.2 *1. id_A è l'applicazione $id_A : A \to A$ tale che $id_A(a) = a$ per ogni $a \in A$, detta identità su A.*

2. $\pi_1 : A \times B \to A$ tale che $\pi_1(a, b) = a$ è detta proiezione sul primo fattore. Analogamente si definisce $\pi_2 : A \times B \to B$, la proiezione sul secondo fattore.

3. $f : \mathbb{R} \to \mathbb{R}$ tale che $f(x) = x^3$ per ogni $x \in \mathbb{R}$.

Definizione 1.3.3 *Una applicazione $f : A \to B$ si dice* iniettiva *se, per ogni $a_1, a_2 \in A$:*

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)\,.$$

Una funzione è iniettiva se, in altre parole, associa ad elementi diversi di A elementi diversi di B.

La 1) e la 3) degli esempi 1.3.2 sono iniettive.

Definizione 1.3.4 *Una applicazione $f : A \to B$ si dice* suriettiva *o* surgettiva *se: per ogni $b \in B$ esiste almeno un elemento $a \in A$ tale che $b = f(a)$. In altre parole, se ogni elemento di B è immagine di qualche elemento di A.*

Gli esempi 1.3.2 sono tutte applicazioni suriettive. La funzione $q : \mathbb{R} \to \mathbb{R}$ tale che $q(x) = x^2$ per ogni $x \in \mathbb{R}$ non lo è.

Definizione 1.3.5 *Una applicazione $f : A \to B$ si dice* biiettiva *o* bigettiva *o* biunivoca *se è sia iniettiva che suriettiva.*

Definizione 1.3.6 *Date due applicazioni $f : A \to B$ e $g : B \to C$, in cui l'insieme d'arrivo della prima sia l'insieme di partenza della seconda, si dice*

prodotto di composizione *o* funzione composta *di* f *e* g *e viene indicata col simbolo* $g \circ f$ *la applicazione* $h : A \to C$ *tale che:*

$$\forall a \in A\,, \quad h(a) = g \circ f(a) = g(f(a))\,.$$

In altri termini, $g \circ f$ *associa all'elemento* a *di* A *l'elemento* c *di* C *che la* g *associa a* $f(a) \in B$*.*

È chiaro dalla definizione, che $g \circ f \neq f \circ g$. Anzi in generale accade che una delle due scritture non abbia senso in quanto il dominio della seconda funzione deve coincidere col codominio della prima. Ma anche quando questo è possibile, le due funzioni, tranne casi particolari, continuano a non coincidere.

Esempio 1.3.7 *Se* $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x$ *e* $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \sin x$*, allora* $g \circ f(x) = \sin(2x)$ *e* $f \circ g(x) = 2 \sin x$*. Le due funzioni sono distinte.*

Definizione 1.3.8 *Data un'applicazione* $f : A \to B$*, l'applicazione* $g : B \to A$ *si dice* inversa *della* f *se*

$$g \circ f = id_A \text{ e } f \circ g = id_B\,.$$

L'applicazione inversa della f, se esiste, si indica con f^{-1}.

Proposizione 1.3.9 *Una applicazione* $f : A \to B$ *ammette inversa se e solo se è biunivoca.*

Dim. Supponiamo che f sia biunivoca. Allora costruiamo la funzione $g : B \to A$ nel seguente modo. Sia $b \in B$. Poiché f è suriettiva, esiste un elemento $a \in A$ tale che $f(a) = b$. Poiché f è iniettiva tale elemento a è unico. Allora definiamo $g(b) = a$. Abbiamo che g è l'inversa di f. Infatti:

$$f \circ g(b) = f(g(b)) = f(a) = b\,, \quad g \circ f(a) = g(f(a)) = g(b) = a\,.$$

Viceversa, supponiamo che esista l'inversa f^{-1} di f. Siano $a_1, a_2 \in A$ tali che $a_1 \neq a_2$. Se fosse $f(a_1) = f(a_2)$, allora anche $f^{-1}(f(a_1)) = f^{-1}(f(a_2))$. Ma $f^{-1} \circ f = id$, quindi si avrebbe $a_1 = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = a_2$. Assurdo, quindi f è iniettiva.
Sia b un generico elemento di B, e sia $a = f^{-1}(b) \in A$. Poiché $f \circ f^{-1} = id_B$, $b = f(f^{-1}(b)) = f(a)$. Quindi esiste un $a \in A$ tale che $b = f(a)$ e dunque f è suriettiva. $\square$

1.4 Cardinalità

Definizione 1.4.1 *Due insiemi A e B si dicono* equipotenti *se esiste una applicazione $f : A \to B$ biunivoca.*

Questa definizione formalizza il concetto di insiemi che hanno lo stesso numero di elementi. In effetti, contare gli elementi di un insieme significa metterlo in corrispondenza biunivoca con un sottoinsieme dei numeri naturali.

Definizione 1.4.2 *La classe di tutti gli insiemi equipotenti ad un dato insieme A si chiama* cardinalità *di A, indicata con $Card(A)$.*

Si può anche definire che $Card(A) \leq Card(B)$ se esiste $f : A \to B$ iniettiva.

Teorema 1.4.3 (Cantor-Bernstein) *Se A e B sono due insiemi per cui $Card(A) \leq Card(B)$ e $Card(B) \leq Card(A)$, allora $Card(A) = Card(B)$, ossia i due insiemi sono equipotenti.*

La dimostrazione di questo, tutt'altro che ovvia, consiste nel far vedere che, se esistono $f : A \to B$ e $g : B \to A$, entrambe iniettive, allora esiste necessariamente $h : A \to B$ biunivoca.

Queste definizioni mostrano degli strani fenomeni quando si ha a che fare con insiemi infiniti. Ad esempio, l'insieme $\mathbb{N}$ dei numeri naturali e l'insieme $\mathbf{P}$ dei numeri pari sono equipotenti; infatti, l'applicazione $D : \mathbb{N} \to \mathbf{P}$ tale che $D(n) = 2n$ è biunivoca. Si ha che un insieme ha la stessa cardinalità di un suo sottoinsieme proprio. È possibile dimostrare che anche $\mathbb{N}$ e l'insieme $\mathbb{Q}$ dei numeri razionali sono equipotenti. In generale, un insieme è infinito se ha la stessa cardinalità di un suo sottoinsieme proprio.

Questa definizione non deve trarre in inganno. Non tutti gli insiemi infiniti sono equipotenti. Ad esempio, $\mathbb{N}$ e $\mathbb{R}$ non hanno la stessa cardinalità. La dimostrazione di ciò si basa sul seguente teorema, che mostra l'esistenza di infiniti esempi di insiemi infiniti con cardinalità via via crescenti.

Teorema 1.4.4 *Sia A un insieme e sia $\mathcal{P}(A)$ l'insieme delle parti di A, cioè l'insieme che ha come elementi tutti i possibili sottoinsiemi di A. Allora, A e $\mathcal{P}(A)$ non sono equipotenti.*

Dim. Supponiamo che, per assurdo, esista $f : A \to \mathcal{P}(A)$ biunivoca. La f associa ad ogni elemento $a \in A$ l'elemento $f(a) \in \mathcal{P}(A)$. Ossia, $f(a)$ è

un sottoinsieme di A. È dunque lecito chiedersi se $a \in f(a)$ oppure no. Per qualche a ciò accadrà, per altri no. Prendiamo in considerazione l'insieme

$$X = \{a \in A \mid a \notin f(a)\} .$$

Questo è un sottoinsieme di A, quindi $X \in \mathcal{P}(A)$. Poiché per ipotesi f era biunivoca, essa è anche suriettiva e quindi, per ipotesi, esiste un elemento $x \in A$ tale che $X = f(x)$. Domanda: $x \in X$? Se $x \in X = f(x)$, per come è definito X dovrebbe essere $x \notin X$. Viceversa, se $x \notin X$, allora, sempre per come è definito X, l'elemento x vi dovrebbe appartenere. Assurdo. L'assurdità sta nell'aver supposto l'esistenza di una f suriettiva. □

1.5 Operazioni e strutture algebriche

Se si guarda con attenzione alle elementari operazioni di somma e prodotto tra numeri interi, si può schematizzarle pensando che esse sono funzioni che ad ogni coppia di operandi associano un elemento che viene detto risultato. Più in astratto, allora, possiamo dare la seguente definizione:

Definizione 1.5.1 *Si dice* operazione binaria interna *sull'insieme non vuoto A una qualsiasi funzione $* : A \times A \to A$. Per comodità scriveremo $a * b$ anziché $*((a, b))$. Un insieme dotato di una o più operazioni viene detto* struttura algebrica*.*

Molte delle operazioni interessanti in matematica hanno alcune proprietà lo studio delle quali è particolarmente significativo. Le strutture algebriche che hanno certe proprietà hanno un nome particolare.

Definizione 1.5.2 *Un insieme A dotato di una operazione interna $*$ si dice* gruppo *se valgono le seguenti proprietà:*

g1. Proprietà associativa:

$$(a * b) * c = a * (b * c) \qquad \forall a, b, c \in A .$$

g2. Esistenza dell'elemento neutro:

$$\exists e \in A \text{ tale che } a * e = e * a = a \quad \forall a \in A .$$

L'elemento e viene detto elemento neutro *di A.*

g3. Esistenza dell'opposto:

$$\forall a \in A \exists a' \in A \text{ tale che } a * a' = a' * a = e\,.$$

L'elemento a' viene detto opposto *di a.*

Se inoltre vale la seguente:

g4. Proprietà commutativa:

$$a * b = b * a \qquad \forall a, b \in A\,,$$

il gruppo A viene detto commutativo o abeliano .

Sono gruppi abeliani $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Vedremo altri esempi di gruppi abeliani.

Vedremo piú aventi un insieme di gruppo non abeliano (l'insieme delle matrici quadrate invertibili con il prodotto righe per colonne).

Definizione 1.5.3 *Un sottoinsieme H di un gruppo G si dice sottogruppo se la restrizione dell'operazione di G fornisce un'operazione interna di H con la quale H risulta esso stesso un gruppo. Questo equivale a dire che:*

1. *il prodotto di due elementi di H è un elemento di H;*
2. *l'inverso di un elemento di H è un elemento di H.*

Ad esempio $\mathbb{Z}$ è un sottogruppo di $\mathbb{R}$, dove l'operazione è chiaramente la somma.

Definizione 1.5.4 *Un insieme A dotato di due operazioni interne $*$ e $\otimes$ si dice* anello *con identità (o unitario) se:*

a1. A è un gruppo abeliano rispetto alla prima operazione $*$.

a2. L'operazione $\otimes$ è associativa:

$$(a \otimes b) \otimes c = a \otimes (b \otimes c) \qquad \forall a, b, c \in A\,.$$

a3. Esiste l'elemento neutro per $\otimes$:

$$\exists u \in A \text{ tale che } a \otimes u = u \otimes a = a \qquad \forall a \in A\,.$$

a4. Valgono le proprietà distributive della $\otimes$ rispetto alla operazione $*$:
$a \otimes (b * c) = (a \otimes b) * (a \otimes c)$ *(distributività a sinistra),*
$(b * c) \otimes a = (b \otimes a) * (c \otimes a)$ *(distributività a destra).*

Se vale anche:

a5. Proprietà commutativa di $\otimes$:

$$a \otimes b = b \otimes a \qquad \forall a, b \in A\,,$$

l'anello A si dice commutativo.

Osserviamo che gli assiomi di anello richiedono che $*$ sia sempre commutativa.

Definizione 1.5.5 *Un insieme A dotato di due operazioni interne $*$ e $\otimes$ si dice* campo *se:*

c1. A è un anello (unitario) commutativo.

c2. Esistenza dell'inverso per l'operazione $\otimes$: $\forall a \in A$, $a \neq e$ (con e elemento neutro di $*$) $\exists a^{-1} \in A$ tale che: $a * a^{-1} = a^{-1} * a = u$ (con u elemento neutro di $\otimes$). L'elemento a^{-1} viene detto inverso *di a.*

Sono campi $\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p$ con p numero primo.

Queste definizioni non esauriscono certo la lista delle strutture algebriche generalmente studiate in matematica. Ve ne sono di più povere, cioè le cui operazioni hanno meno proprietà, ad esempio il *semigruppo*, una struttura la cui operazione gode delle proprietà g1, g2, ma non g3, manca cioè l'opposto. Tale è l'insieme $\mathbb{N}$ dei numeri naturali. Ma ve ne sono anche di più ricche alcune di queste saranno oggetto di uno studio più approfondito più avanti.

È interessante anche studiare le applicazioni tra strutture algebriche dello stesso tipo che, in un certo senso, conservino le operazioni.

Definizione 1.5.6 *Date due strutture algebriche dello stesso tipo G e H, una applicazione $f : G \to H$ è un* morfismo *se, per ogni operazione $*$ su G vi è una corrispondente operazione $\otimes$ su H tale che:*

$$f(g_1 * g_2) = f(g_1) \otimes f(g_2) \qquad \forall g_1, g_2 \in G\,.$$

In altre parole, f è un morfismo se eseguire una operazione su G e poi applicare la f al risultato è la stessa cosa che eseguire la corrispondente operazione su H tra le immagini degli operandi dati. Un morfismo biunivoco si dice *isomorfismo*. Un morfismo tra gruppi si dice *omomorfismo*.

1.6 I numeri complessi

L'insieme dei numeri complessi, indicato con $\mathbb{C}$, è una estensione dell'insieme dei numeri reali, all'interno della quale è sempre possibile estrarre radici quadrate, anche di numeri negativi. Anzi, questa condizione, cioè l'esistenza delle radici quadrate, determina come diretta conseguenza la possibilità di avere tutte le radici di equazioni algebriche e l'esistenza dei logaritmi. Inoltre, la teoria delle funzioni di variabile complessa, alquanto diversa da quella della analisi reale, è estremamente efficace nel descrivere svariati fenomeni fisici e matematici. Ma questa è un'altra storia.

Per noi un numero complesso sarà un oggetto del tipo $a+ib$ dove a, b sono numeri reali e i è un simbolo detto unità immaginaria non meglio specificato.

Se $z \in \mathbb{C}$, $z = a + ib$, a viene detta *parte reale* di z e indicata con $\Re(z)$, mentre b è detta *parte immaginaria* e indicata con $\Im(z)$.

Su $\mathbb{C}$ si possono definire due operazioni che daranno a $\mathbb{C}$ la struttura di campo, poiché verificano tutte le proprietà richieste.

Somma. Se $z = a + ib$ e $w = c + id$, la loro somma $z + w$ è così definita:

$$z + w = (a + c) + i(b + d)\,.$$

Quindi, per definizione, la somma tra due numeri complessi è il numero che ha come parte reale la somma (vista come operazione sui numeri reali) delle parti reali dei due addendi e come parte immaginaria, la somma delle parti immaginarie.

Lunghe verifiche, lasciate come esercizio a chi non ci crede, dimostrano che $\mathbb{C}$, con questa operazione di somma, è un gruppo abeliano.

Prodotto. Se $z = a + ib$ e $w = c + id$, il loro prodotto $z \cdot w$ (indicato anche con zw) è così definito:

$$z \cdot w = (ac - bd) + i(ad + bc)\,.$$

Esercizio 1.6.1 *Eseguire* $(2 + 2i) \cdot (1 + 3i)$.

Osservazione 1.6.2

1. *Il numero complesso 0 (a rigore* $0 + 0i$*) è l'elemento neutro della somma.*

2. *Il numero complesso 1 (a rigore* $1+0i$*) è l'elemento neutro del prodotto.*

3. *Se scriviamo semplicemente a per* $a + 0i$, *possiamo identificare* $\mathbb{R}$ *con il sottoinsieme dei numeri complessi con parte immaginaria nulla e, in questo senso, pensare* $\mathbb{R} \subseteq \mathbb{C}$.

4. *Il numero complesso i (a rigore* $0 + 1i$*) è tale che* $ii = i^2 = -1$. *In questo senso,* $\sqrt{-1} = i$ *oppure* $-i$. *Infatti,* $i^2 = (-i)^2 = -1$.

5. *Se* $z \in \mathbb{C}$, $z = a + ib$, $z \neq 0$ *(ossia, a ≠0 oppure* $b \neq 0$*), sia:*

$$w = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}\,.$$

   È facile verificare che $z \cdot w = 1$ *quindi* $w = z^{-1}$ *e* $\mathbb{C}$ *è un campo.*

Definizione 1.6.3 *Dato* $z \in \mathbb{C}$, $z = a + ib$, *il numero reale non negativo* $\sqrt{a^2 + b^2}$ *si dice* modulo *di z e si indica con* $|z|$.

Osservazione 1.6.4 1. $|z| \geq 0$ *per ogni* $z \in \mathbb{C}$.

2. $|z| = 0$ *se e solo se* $z = 0$.

3. $|zw| = |z||w|$ *ovvero, il modulo del prodotto è uguale al prodotto dei moduli.*

Introduciamo ora una operazione su $\mathbb{C}$ ad un solo operando (operazione unaria) detta *coniugio*.

Definizione 1.6.5 *Se* $z = a + ib \in \mathbb{C}$, *si definisce* coniugato *di z (e si indica con* $\bar{z}$*) il numero complesso* $\bar{z} = a - ib$. *Ovverosia,* $\Re(z) = \Re(\bar{z})$, *mentre* $\Im(z) = -\Im(\bar{z})$.

Osservazione 1.6.6 *Il coniugio, rispetto alle operazioni di* $\mathbb{C}$, *ha le seguenti proprietà:*

1. $\overline{(z + w)} = \bar{z} + \bar{w}$.

2. $\overline{(z \cdot w)} = \bar{z} \cdot \bar{w}$.

3. $|\bar{z}| = |z|$.

4. $z = \bar{z}$ *se e solo se* $z \in \mathbb{R}$.

5. $z \cdot \bar{z} = |z|^2$.

6. $z^{-1} = \frac{\bar{z}}{|z|^2}$ *(supposto* $z \neq 0$*)*.

7. $z + \bar{z} = 2\Re(z)$; $\qquad z - \bar{z} = 2i\Im(z)$.

Chi avesse difficoltà ad accettare locuzioni come "oggetto del tipo $a+ib$", può fare così: può considerare su $\mathbb{R} \times \mathbb{R}$ le seguenti operazioni:
Somma (indicata con $+$): $\quad (a,b) + (c,d) = (a+c, b+d)$.
Prodotto (indicato con $\cdot$): $\quad (a,b) \cdot (c,d) = (ac - bd, ad + bc)$.
Con queste operazioni $\mathbb{R} \times \mathbb{R}$ è un campo isomorfo a $\mathbb{C}$. Tale isomorfismo, che associa a $z \in \mathbb{C}$, $z = a + ib$, la coppia $(a,b) \in \mathbb{R} \times \mathbb{R}$, fornisce la rappresentazione dei complessi come punti del piano cartesiano, che in questo contesto viene detto *piano di Gauss*.

Per il calcolo delle radici di polinomi, è molto utile la rappresentazione *trigonometrica* dei numeri complessi, che corrisponde a porre nel piano, anziché le coordinate cartesiane, le coordinate polari.

Se $z = a + ib$ e $z \neq 0$, possiamo scrivere $z = |z|(\frac{a}{|z|} + i\frac{b}{|z|})$. Fin qui nulla di strano. Posto $\alpha = \frac{a}{|z|}$ e $\beta = \frac{b}{|z|}$, si ha che $\alpha^2 + \beta^2 = 1$ e, pertanto, esiste un unico ω, $0 \leq \omega < 2\pi$ e tale che $\alpha = \cos\omega$ e $\beta = \sin\omega$. L'angolo ω è detto *argomento* del numero complesso z. Se poniamo $|z| = \exp(t)$, con $t \in \mathbb{R}$, allora possiamo scrivere $z = \exp(t)(\cos\omega + i\sin\omega)$. L'angolo ω si indica anche con $arg(z)$.

Osservazione 1.6.7 *Se z e w sono numeri complessi non nulli, si ha che $arg(zw) = arg(z) + arg(w)$. L'argomento del prodotto è uguale alla somma degli argomenti. Ciò si dimostra con le formule di addizione trigonometriche.*

Capitolo 2

POLINOMI ED EQUAZIONI ALGEBRICHE

2.1 Polinomi

Definizione 2.1.1 *Si dice* polinomio *nella indeterminata x a coefficienti reali (risp. complessi) ogni oggetto del tipo:*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

dove n è un intero non negativo e gli a_i, detti coefficienti, sono numeri reali (risp. complessi). Un polinomio $p(x)$ si dirà di grado n, *e si scriverà $deg(p) = n$, se $a_n \neq 0$ e $a_k = 0$ per ogni $k > n$.*

Principio di identità dei polinomi. Due polinomi sono uguali se e solo se hanno tutti i coefficienti corrispondenti uguali.

Definizione 2.1.2 *Un polinomio con un solo coefficiente non nullo viene detto* monomio*. Un polinomio con due soli coefficienti non nulli viene detto* binomio *e così via.*

L'insieme dei polinomi a coefficienti reali (risp. complessi) nella indeterminata x viene indicato con $\mathbb{R}[x]$ (risp. $\mathbb{C}[x]$).

Osservazione 2.1.3 *Un numero reale a (non nullo) può essere pensato come un polinomio (di grado zero). I polinomi di grado zero sono detti anche* costanti.

Il polinomio che ha tutti i coefficienti uguali a zero viene detto *polinomio nullo*, si indica con 0 e può essere identificato con il numero reale 0. Il grado di 0 verrà specificato in seguito.

Su $\mathbb{R}[x]$ possiamo definire due operazioni.

Somma. Siano $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ e $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ due polinomi e supponiamo che sia $n \geq m$. Allora il polinomio somma $h(x) = p(x) + q(x)$ è così definito:

$$h(x) = a_n x^n + \cdots + a_{m+1}x^{m+1}x^{m+1} + (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + a_0 + b_0 \,.$$

Il polinomio somma è il polinomio che ha come coefficienti la somma dei coefficienti dei termini di ugual grado.

Proposizione 2.1.4 $\mathbb{R}[x]$ *con l'operazione somma è un gruppo abeliano di cui il polinomio nullo è l'elemento neutro.*

Prodotto. Se $p(x) = a_n x^n$ e $q(x) = b_m x^m$, allora $p(x)q(x) = a_n b_m x^{n+m}$. Inoltre vale, per definizione, la proprietà distributiva del prodotto rispetto alla somma. In questo modo è ben definito il prodotto tra due qualsiasi polinomi.

Esempio 2.1.5 $(3x^3 + 2x^2 - x + 1)(2x^2 - x + 2) = 6x^5 + 4x^4 - 2x^3 + 2x^2 - 3x^4 - 2x^3 + x^2 - x + 6x^3 + 4x^2 - 2x + 2 = 6x^5 + x^4 + 2x^3 + 7x^2 - 3x + 2.$

Proposizione 2.1.6 *Con le due operazioni di somma e prodotto,* $\mathbb{R}[x]$ *risulta essere un anello commutativo con identità. L'identità è il polinomio* 1*, polinomio di grado zero.*

Osservazione 2.1.7 *Siano* p *e* q *due polinomi non nulli. Allora:*
1) $\deg(pq) = \deg(p) + \deg(q)$.
2) $deg(p + q) \leq \max\{\deg(p), deg(q)\}$.
Cioè, il grado del prodotto è uguale alla somma dei gradi dei fattori, mentre il grado della somma non può superare il più grande tra i gradi degli addendi, ma di più non si può dire.

Esempio 2.1.8 *Se* $p = x^5 + x^4 - 3x^3 + 2x^2 + 1$, $q = -x^5 - x^4 + 3x^3 - 2x^2 - x$, *allora* $\deg(p) = 5$, $\deg(q) = 5$, *ma* $p + q = -x + 1$, *e dunque* $deg(p + q) = 1$.

Affinché la proprietà 1) valga senza eccezioni, di solito si definisce

$$\deg(0) = -\infty\,.$$

Osservazione 2.1.9 $\mathbb{R}[x]$ *non è un campo. Infatti se p è un polinomio tale che* $\deg(p) > 0$ *e $q \neq 0$, allora $deg(pq) > 0$ e dunque non potrà mai essere $pq = 1$, perché, appunto* $\deg(1) = 0$*. Quindi i polinomi di grado positivo non ammettono inverso.*

2.2 Divisione tra polinomi

Vi è una straordinaria somiglianza tra $\mathbb{R}[x]$ e $\mathbb{Z}$, l'anello degli interi. Entrambi sono anelli commutativi con identità, ma non campi. Vogliamo estendere ancora di più la somiglianza delle proprietà formali introducendo una operazione di divisione con resto anche sui polinomi.

Definizione 2.2.1 *Diremo che il polinomio $d(x)$* divide *il polinomio $p(x)$, se esiste un polinomio $q(x)$ tale che risulti $p(x) = q(x) \cdot d(x)$. In tal caso si scrive anche $d\,|\,p$.*

Purtroppo, dati p e d non sempre esiste un siffatto q. Ad esempio il polinomio x non divide $x^2 + 1$. Infatti, per questioni di grado, $\deg(q) = 1$. Quindi $q(x) = ax + b$. Ma $q \cdot x = ax^2 + bx$ che per nessun valore dei coefficienti a e b può essere uguale a $x^2 + 1$.

In generale è però possibile effettuare la *divisione con resto* tra polinomi, in maniera analoga a quella tra numeri interi.

Proposizione 2.2.2 *Dati due polinomi p e d esistono e sono univocamente determinati due polinomi q ed r (detti rispettivamente quoziente e resto della divisione) tali che:*

1. $p = q \cdot d + r$,
2. $deg(r) < \deg(d)$.

Dimostriamo l'unicità. Supponiamo che $p = q_1 \cdot d + r_1$ e anche $p = q_2 \cdot d + r_2$. Allora: $(q_1 \cdot d + r_1) - (q_2 \cdot d + r_2) = 0$ e quindi $(q_1 - q_2) \cdot d = r_2 - r_1$. Se fosse $q_1 - q_2 \neq 0$ si avrebbe: $\deg((q_1 - q_2) \cdot d) \geq \deg(d) > \max\{\deg(r_2), \deg(r_1)\} \geq$

$\deg(r_1 - r_2)$ e dunque non vi potrebbe essere l'uguaglianza. Quindi $q_1 = q_2$. Ma allora anche $r_1 - r_2 = 0$ e quindi anche $r_1 = r_2$.

Alla determinazione di $q(x)$ e $r(x)$ si giunge attraverso un algoritmo, detto *algoritmo di Euclide*, che illustriamo con un esempio.

Siano $p(x) = 3x^5 + 2x^4 - 2x^3 + x - 1$ e $d(x) = 2x^2 + 2x + 1$. Vogliamo eseguire la divisione.

$$\begin{array}{l|l} 3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2} & \end{array}$$

1^o passo. Sia m_1 il monomio tale che il primo termine di $d(x)$ moltiplicato per m_1 dia il primo termine di $p(x)$; nello specifico, $2x^2 \cdot m_1 = 3x^5$, dunque $m_1 = \frac{3}{2}x^3$. Scriviamo m_1 sotto $d(x)$.

$$\begin{array}{l|l} 3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2} & \frac{3}{2}x^3 \end{array}$$

2^o passo. Calcoliamo $d \cdot m_1$, scriviamo $-d \cdot m_1$ sotto $p(x)$ ed eseguiamo la somma indicando con $p_1 = p - d \cdot m_1$.

Nel nostro caso $-d \cdot m_1 = -3x^5 - 3x^4 - \frac{3}{2}x^3$ e $p_1 = -x^4 - \frac{3}{2}x^3 + 0x^2 + x - 1$.

$$\begin{array}{l|l} 3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2} -3x^5 - 3x^4 - \frac{3}{2}x^3 & \frac{3}{2}x^3 \\ \cline{1-1} -x^4 - \frac{7}{2}x^3 + 0x^2 + x - 1 & \end{array}$$

3^o passo. Adesso si itera il procedimento, prendendo p_1 al posto di p. Sia m_2 il monomio tale che $2x^2 \cdot m_2 = -x^4$.

Nel nostro caso $m_2 = -\frac{1}{2}x^2$. Scriviamo m_2 sotto $d(x)$ sommandolo a m_1.

$$\begin{array}{l|l} 3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2} -3x^5 - 3x^4 - \frac{3}{2}x^3 & \frac{3}{2}x^3 - \frac{1}{2}x^2 \\ \cline{1-1} -x^4 - \frac{7}{2}x^3 + 0x^2 + x - 1 & \end{array}$$

4^o passo. Calcoliamo $d \cdot m_2$, scriviamo $-d \cdot m_2$ sotto p_1 ed eseguiamo la somma indicando con $p_2 = p_1 - d \cdot m_2$.

Nel nostro caso $-d \cdot m_2 = x^4 + x^3 + \frac{1}{2}x^2$ e $p_2 = -\frac{5}{2}x^3 + \frac{1}{2}x^2 + x - 1$.

$$
\begin{array}{l|l}
3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2}
-3x^5 - 3x^4 - \frac{3}{2}x^3 & \frac{3}{2}x^3 - \frac{1}{2}x^2 \\ \cline{1-1}
-x^4 - \frac{7}{2}x^3 + 0x^2 + x - 1 & \\
x^4 + x^3 + \frac{1}{2}x^2 & \\ \cline{1-1}
-\frac{5}{2}x^3 + \frac{1}{2}x^2 + x - 1 &
\end{array}
$$

5^o passo. Calcoliamo m_3 tale che $2x^2 \cdot m_3 = -\frac{5}{2}x^3$. Scriviamo m_3 sotto $d(x)$ sommandolo a $m_1 + m_2$; poi poniamo $p_3 = p_2 - d \cdot m_3$.

Nel nostro caso $m_3 = -\frac{5}{4}x$ e quindi $-d \cdot m_3 = \frac{5}{2}x^3 + \frac{5}{2}x^2 + \frac{5}{4}x$ e $p_3 = p_2 - d \cdot m_3 = 3x^3 + \frac{9}{4}x - 1$.

$$
\begin{array}{l|l}
3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2}
-3x^5 - 3x^4 - \frac{3}{2}x^3 & \frac{3}{2}x^3 - \frac{1}{2}x^2 - \frac{5}{4}x \\ \cline{1-1}
-x^4 - \frac{7}{2}x^3 + 0x^2 + x - 1 & \\
x^4 + x^3 + \frac{1}{2}x^2 & \\ \cline{1-1}
-\frac{5}{2}x^3 + \frac{1}{2}x^2 + x - 1 & \\
\frac{5}{2}x^3 + \frac{5}{2}x^2 + \frac{5}{4}x & \\ \cline{1-1}
3x^2 + \frac{9}{4}x - 1 &
\end{array}
$$

6^o passo. Calcoliamo m_4 tale che $2x^2 \cdot m_4 = 3x^2$. Scriviamo m_4 sotto $d(x)$ sommandolo a $m_1 + m_2 + m_3$; poi poniamo $p_4 = p_3 - d \cdot m_4$.

Nel nostro caso $m_4 = \frac{3}{2}$ e quindi $-d \cdot m_4 = -3x^2 - 3x - \frac{3}{2}$ e $p_4 = p_3 - d \cdot m_4 = -\frac{3}{4}x - \frac{5}{2}$.

$$
\begin{array}{l|l}
3x^5 + 2x^4 - 2x^3 + 0x^2 + x - 1 & 2x^2 + 2x + 1 \\ \cline{2-2}
-3x^5 - 3x^4 - \frac{3}{2}x^3 & \frac{3}{2}x^3 - \frac{1}{2}x^2 - \frac{5}{4}x + \frac{3}{2} \\ \cline{1-1}
-x^4 - \frac{7}{2}x^3 + 0x^2 + x - 1 & \\
x^4 + x^3 + \frac{1}{2}x^2 & \\ \cline{1-1}
-\frac{5}{2}x^3 + \frac{1}{2}x^2 + x - 1 & \\
\frac{5}{2}x^3 + \frac{5}{2}x^2 + \frac{5}{4}x & \\ \cline{1-1}
3x^2 + \frac{9}{4}x - 1 & \\
-3x^2 - 3x - \frac{3}{2} & \\ \cline{1-1}
-\frac{3}{4}x - \frac{5}{2} &
\end{array}
$$

7^o passo. Poiché p_4 ha grado minore di d, il procedimento si interrompe e si ha che: $r(x) = p_4(x)$ e inoltre $q(x) = m_1 + m_2 + m_3 + m_4$.

Possiamo verificare che $p(x) = d(x)(m_1 + m_2 + m_3 + m_4) + p_4(x)$.

In generale, l'algoritmo di Euclide consiste nel costruirsi una successione di polinomi p_i con $p_0 = p$, il dividendo, e $p_i = p_{i-1} - d \cdot m_i$ dove $m_i = \frac{a_{k_i}}{b_m} x^{k_i - m}$ con a_{k_i} il primo coefficiente del termine di massimo grado di p_i, $\deg(p_i) = k_i$, e b_m il primo coefficiente di d, $\deg(d) = m$.

Si può vedere che $\deg(p_i) > \deg(p_{i+1})$ e quindi dopo un numero finito di passi, per un opportuno indice h, $\deg(p_{h-1}) \geq \deg(d) > \deg(p_h)$. Allora, ponendo $r(x) = p_h(x)$ e $q(x) = m_1 + \cdots + m_h$, abbiamo che $r(x)$ e $q(x)$ sono il resto e il quoziente cercati, cioè $p(x) = q(x)d(x) + r(x)$ e $deg(r) < \deg(d)$.

2.3 Radici di polinomi

Sia $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ un polinomio a coefficienti reali. A p posso associare una funzione da $\mathbb{R}$ in $\mathbb{R}$ che all'elemento c associa il numero reale $a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0$ che si ottiene sostituendo c al posto della indeterminata x ed eseguendo poi le operazioni tra numeri reali.

Esempio 2.3.1 *Dato* $p(x) = 2x^3 + x^2 - x + 4$*, si ha che:* $p(1) = 2 + 1 - 1 + 4 = 6$, $\quad p(0) = 4$, $\quad p(-2) = 2(-8) + (4) - (-2) + 4 = -6$.

Definizione 2.3.2 *Il numero reale (o complesso) c si dice* radice *del polinomio* $p(x) = a_n x^n + a_{n-1} x_{n-1} + \cdots + a_1 x + a_0$ *se* $p(c) = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0 = 0$.

Ossia, se sostituendo c alla indeterminata x si ottiene 0.

Esempio 2.3.3 *Sia* $p = 2x^4 + 3x^3 - x^2 + x - 2$. *Il numero reale -2 è radice di p. Infatti,* $2(-2)^4 + 3(-2)^3 - (-2)^2 + (-2) - 2 = 32 - 24 - 4 - 2 - 2 = 0$. *Il numero reale 1 non è radice di p. Sostituendo, si ha* $p(1) = 3 \neq 0$.

Teorema 2.3.4 (Ruffini) *Sia $p(x)$ un polinomio. Il numero c è radice di p se e solo se il polinomio $(x - c)$ divide $p(x)$.*

Dim. Supponiamo che $(x - c)$ divida $p(x)$ ossia che esista $q(x)$ tale che $p(x) = q(x) \cdot (x - c)$. Sostituendo c al posto della x, si ha che: $p(c) = q(c)(c - c) = q(c)0 = 0$. Quindi c è una radice di p.

Viceversa, supponiamo che c sia radice di p, cioè che $p(c) = 0$. Eseguiamo la divisione con resto di p per $(x - c)$. Troveremo due polinomi $q(x)$ e $r(x)$ tali che $p = q(x-c)+r$. Ma, poiché deve essere che $\deg(r) < \deg(x-c) = 1$, $\deg(r) \leq 0$ e quindi r è una costante. Sostituendo c al posto della x, si ha: $p(c) = q(c)(c - c) + r$. Poiché per ipotesi $p(c) = 0$, allora $r = 0$ e quindi p è divisibile per $(x - c)$. □

Osservazione 2.3.5 *Un polinomio di grado 1 ha una e una sola soluzione. Infatti se $p(x) = ax + b$ (con $a \neq 0$) il numero $-\frac{b}{a}$ è radice di p. Viceversa, se c è radice di p, cioè $p(c) = 0$, allora necessariamente $c = -\frac{b}{a}$.*

Osservazione 2.3.6 *Se c è radice di p e p si scrive come prodotto di due polinomi q e s, allora c è radice di almeno uno dei due fattori. Infatti, se per assurdo c non fosse radice né di q né di s, allora $q(c) \neq 0$ e anche $s(c) \neq 0$, da cui anche $p(c) = q(c)s(c) \neq 0$. Questo ci dice anche che, se $R(p)$ è l'insieme delle radici di $p = qs$, allora $R(p) = R(q) \cup R(s)$.*

Come immediata conseguenza del Teorema di Ruffini possiamo a priori definire un limite superiore al numero di radici possedute da un polinomio.

Proposizione 2.3.7 *Sia $p(x)$ un polinomio di grado $n \geq 0$ (quindi non nullo). Allora p ha al più n radici.*

Dim. Dimostriamolo per induzione sul grado n del polinomio. L'Osservazione 2.3.5 ci garantisce che per $n = 1$ l'ipotesi è verificata. Supponiamo ora che ciò sia vero per tutti i polinomi di grado $n - 1$, e dimostriamo che ciò sia vero anche per tutti i polinomi di grado n. Sia p di grado n. Se non ha radici, amen. La tesi vale. Se ha almeno una radice c, allora per il Teorema di Ruffini, $p = q \cdot (x-c)$. Per l'Osservazione 2.3.5, $(x-c)$ ha una sola radice. Per ipotesi induttiva q, che ha grado $n - 1$, ha al più $n - 1$ radici. Siccome l'insieme delle radici di p è uguale all'unione dell'insieme delle radici di q, che ha al più $n - 1$ elementi, con le radici di $(x - c)$, che ne ha una sola, p avrà al più n radici. □

Osservazione 2.3.8 *Se un polinomio ha infinite radici, è il polinomio nullo. Inoltre, dati p e q polinomi di grado (al più) n, se esistono $n + 1$ numeri c_i, distinti a due a due, tali che $p(c_i) = q(c_i)$ per ogni $i = 1, \ldots, n + 1$, allora*

$p = q$. Infatti, i c_i sono radici del polinomio $p - q$, che dovrebbe avere grado minore o uguale a n. Se quindi fosse non nullo, dovrebbe avere al più n radici, ma siccome di radici ne ha $n + 1$, $p - q$ è il polinomio nullo e dunque $p = q$.

Consideriamo il seguente esempio. Sia $p(x) = (x - 1)^2$ e $q(x) = x - 1$. Essi hanno entrambi la stessa radice 1, ma in un certo qual senso p ci sembra più simile a $x^2 - 1 = (x + 1)(x - 1)$ che di radici ne ha due. Ci piacerebbe poter dire che anche $p(x)$ ha due radici, $x = 1$ contata due volte. Queste considerazioni motivano la seguente definizione.

Definizione 2.3.9 *Sia c una radice del polinomio $p(x)$. Se $(x - c)^m$ divide $p(x)$, con m intero positivo, ma $(x - c)^{m+1}$ non divide p, allora diremo che $(x - c)^m$* divide esattamente *p e che c ha* molteplicità *m.*

Se la molteplicità di c è 1, allora c viene detta radice semplice*.*

Esempio 2.3.10 *Sia $p = x^4 - 2x^3 + 2x - 1$. Dico che 1 è una radice di p che ha molteplicità 3. Infatti $p = (x - 1)^3(x + 1)$, se si esegue la divisione, mentre $p = (x - 1)^4 + (2x^3 - 6x^2 + 6x - 2)$ e dunque non è divisibile per $(x - 1)^4$.*

D'altra parte, non è detto che un polinomio ammetta sempre delle radici. Ad esempio $x^2 + 1$ non ammette nessuna radice reale, perché nessun numero reale al quadrato può dare -1. Pensato come elemento di $\mathbb{C}[x]$, il polinomio in questione ha come radice l'unità immaginaria i. Infatti $(i)^2 + 1 = -1 + 1 = 0$.

Il campo dei numeri complessi ha, da questo punto di vista, le migliori proprietà. Vale, infatti, il seguente fondamentale risultato (di cui è fuori luogo dare una dimostrazione in questo libro).

Teorema 2.3.11 *Un polinomio $p \in \mathbb{C}[x]$ di grado n ammette esattamente n radici, contate con la loro molteplicità.*

Contate con la loro molteplicità vuol dire che, se ad esempio un polinomio ha una radice di molteplicità 2 ed un'altra di molteplicità 3, diremo che ha cinque radici.

Proposizione 2.3.12 *Se un polinomio $p \in \mathbb{R}[x]$ ammette c come radice, allora anche $\bar{c}$ è radice di p e con la stessa molteplicità di c.*

Dim. Siccome p ha tutti i coefficienti reali, $p(\bar{c}) = \overline{p(c)} = \bar{0} = 0$. Quindi $\bar{c}$ è radice di p. Inoltre sia k la molteplicità di c e supponiamo sia $h < k$ la molteplicità di $\bar{c}$. Allora si ha che $p(x) = (x-c)^h(x-\bar{c})^h q(x)$. Ma: $(x-c)^h(x-\bar{c})^h = (x^2 - 2(\Re(c))x + |c|^2)^h$, che è un polinomio a coefficienti reali. Quindi $q(x)$ risulta essere anche esso un polinomio a coefficienti reali che ha c tra le sue radici ma non $\bar{c}$. Ciò è assurdo per quanto visto prima. Analogamente, si ha l'assurdo se si suppone $k < h$. Quindi $k = h$. □

2.4 Radici dell'unità

Consideriamo l' equazione:

$$x^n = 1\,. \tag{2.1}$$

Questa equazione di grado n ha sempre $x = 1$ come soluzione e, se n è pari, anche $x = -1$. Ma il teorema fondamentale dell'algebra ci dice che essa di soluzioni ne ha n. Cerchiamo di determinarle tutte. Le soluzioni della (2.1) sono dette radici n-esime dell'unità.

Scriviamo $x \in \mathbb{C}$ in forma trigonometrica:

$$x = \rho(\cos\omega + i\sin\omega)\,.$$

Essendo, per l'Osservazione 1.6.7, l'argomento del prodotto uguale alla somma degli argomenti, $x^n = \rho^n(\cos n\omega + i\sin n\omega)$.

Affinché si abbia $\rho^n(\cos n\omega + i\sin n\omega) = 1$ dovrà risultare:

$$\begin{cases} \rho^n = 1 \\ n\omega = 2k\pi \quad \text{con } k \text{ intero.} \end{cases}$$

Siccome $\rho \in \mathbb{R}^+ = \{r \in \mathbb{R} \mid r \geq 0\}$, $\rho^n = 1$ se e solo se $\rho = 1$. Poiché inoltre $0 \leq \omega < 2\pi$, $\omega = \frac{2k\pi}{n}$, con $k = 0, 1, \ldots, n-1$. Quindi le n radici n-esime dell'unità sono i numeri complessi aventi modulo 1 e argomento $\omega = \frac{2k\pi}{n}$ con $k = 0, 1, \ldots, n-1$.

Esempio 2.4.1 *Determiniamo le tre radici cubiche dell'unità, cioè le soluzioni della equazione $x^3 = 1$.*
Per $k = 0$ si ha $x_1 = 1$.
Per $k = 1$ si ha $x_2 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.
Per $k = 2$ si ha $x_3 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.
Si esegua come esercizio la verifica. Si noti che $x_3 = \bar{x}_2$.

2.5 Soluzioni delle equazioni di 2°, 3° e 4° grado.

La ricerca delle formule risolutive delle equazioni algebriche, cioè di formule che permettessero di trovare le radici di un polinomio, è stata una delle più prolungate e sofferte nella storia della matematica. Iniziata nella notte dei tempi con la scoperta della formula risolutiva dell'equazione generica di 2^o grado, ha compiuto il passo successivo con gli algebristi italiani del '500, approdati alla risoluzione dell'equazione di 3^o grado, e poco dopo, a quella di 4^o grado. L'ultimo tassello lo ha posto Évariste Galois (1811-1832), col suo fondamentale lavoro, stabilendo che la generica equazione di grado superiore al quarto non può essere risolta con un numero finito di operazioni algebriche, come somme, prodotti ed estrazioni di radici. Questo può essere fatto solo nel caso di equazioni particolarmente semplici, e di fatto il determinare radici di polinomi diviene un problema di calcolo numerico.

Indichiamo qui di seguito le formule risolutive per le equazioni di grado fino al quarto.

2.5.1 Equazioni di secondo grado

Consideriamo la generica equazione di secondo grado:

$$x^2 + ax + b = 0\,. \tag{2.2}$$

Le due soluzioni di questa equazione, come è ben noto, sono:

$$x = -\frac{a}{2} + \frac{\sqrt{a^2 - 4b}}{2} \quad \text{e} \quad x = -\frac{a}{2} - \frac{\sqrt{a^2 - 4b}}{2}\,.$$

L' espressione $\Delta = a^2 - 4b$ è detta *discriminante*.

Le due radici sono reali se $\Delta \geq 0$. Se $\Delta < 0$, esse sono complesse coniugate non reali.

2.5.2 Equazioni di terzo grado

Consideriamo la generica equazione di terzo grado:

$$y^3 + ay^2 + by + c = 0\,. \tag{2.3}$$

Per semplificarla introduciamo l'incognita ausiliaria x tale che:

$$y = x - \frac{a}{3}$$

Sostituendo in (2.3), il termine di secondo grado si annulla e la nuova equazione in x diventa:

$$x^3 + px + q = 0\,, \tag{2.4}$$

dove $p = b - \frac{a^2}{3}$ e $q = \frac{2}{27}a^3 - \frac{ab}{3} + c$.

Trovate le soluzioni della (2.4) è poi immediato risalire alle soluzioni della equazione iniziale.

Se poniamo $x = u + v$, la (2.4) diventa:

$$(u + v)^3 + p(u + v) + q = 0\,,$$

ovvero

$$u^3 + v^3 + q + (3uv + p)(u + v) = 0\,.$$

E' evidente che, se determino due numeri u e v tali che:
1) $u^3 + v^3 = -q$,
2) $uv = -\frac{p}{3}$ (che equivale a $u^3v^3 = -\frac{p^3}{27}$),
allora $x = u + v$ è soluzione della (2.4).

Se di due numeri conosco la somma A e il prodotto B, posso facilmente ricavarli in quanto essi sono le soluzioni della equazione di secondo grado $z^2 - Az + B = 0$. Quindi u^3 e v^3 sono le soluzioni della equazione:

$$z^2 + qz - \frac{p^3}{27} = 0\,,$$

cioè

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad \text{e} \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\,.$$

Poiché $x = u + v$, si ha infine:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4}\frac{p^3}{27}}}\,, \tag{2.5}$$

che è la formula definitiva.

Osservazione 2.5.1 *Tra le nove possibili coppie (u, v) bisogna scegliere, per determinare le soluzioni $x = u + v$, le tre tali che si abbia $3uv = -p$.*

2.5.3 Equazioni di quarto grado

Consideriamo la generica equazione di quarto grado:

$$x^4 + ax^3 + bx^2 + cx + d = 0\,. \tag{2.6}$$

Riscriviamola in questo modo:

$$x^4 + ax^3 = -bx^2 - cx - d\,.$$

Aggiungiamo ad entrambi i membri il termine $\frac{a^2}{4}x^2$. Otteniamo:

$$(x^2 + \frac{a}{2}x)^2 = (\frac{a^2}{4} - b)x^2 - cx - d\,.$$

Aggiungendo ancora ad entrambi i membri il termine

$$(x^2 + \frac{a}{2}x)y + \frac{y^2}{4}\,,$$

dove y è una incognita ausiliaria, otteniamo

$$(x^2 + \frac{a}{2}x + \frac{y}{2})^2 = (\frac{a^2}{4} - b + y)x^2 + (\frac{ay}{2} - c)x + (\frac{y^2}{4} - d)\,. \tag{2.7}$$

Vogliamo porre delle condizioni su y affinché il secondo membro della equazione sia un quadrato perfetto. Dato un trinomio $Ax^2 + Bx + C$, questo è un quadrato perfetto se $B^2 - 4AC = 0$. Nel nostro caso

$$(\frac{ay}{2} - c)^2 - 4(\frac{a^2}{4} - b + y)(\frac{y^2}{4} - d) = 0\,. \tag{2.8}$$

Questo accade se e solo se y è soluzione della equazione:

$$y^3 - by^2 + (ac - 4d)y - (d(a^2 - 4b) + c^2) = 0\,. \tag{2.9}$$

Sia y_0 una soluzione di (2.9) determinata usando la risoluzione, descritta in precedenza, delle equazioni di terzo grado. Con questa scelta, il secondo membro della (2.7) è il quadrato di un binomio, quindi:

$$(x^2 + \frac{a}{2}x + \frac{y_0}{2})^2 = (Px + Q)^2\,, \tag{2.10}$$

dove

$$P = \sqrt{\frac{a^2}{4} - b + y_0} \quad \text{e} \quad Q = \sqrt{\frac{{y_0}^2}{4} - d}\,.$$

Siccome la (2.10) è equivalente alla equazione iniziale, le quattro soluzioni di questa sono date dalle soluzioni delle due equazioni di secondo grado equivalenti anch'esse a (2.10):

$$\begin{aligned} x^2 + \frac{a}{2}x + \frac{y_0}{2} &= Ax + B\,, \\ x^2 + \frac{a}{2}x + \frac{y_0}{2} &= -Ax - B\,. \end{aligned}$$

2.6 Regola di Cartesio

Sia $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio di $\mathbb{R}[x]$. Supponiamo che esso abbia tutte le radici reali. Scriviamo nell'ordine tutti i coefficienti di $p(x)$, *omettendo quelli nulli.*

Definizione 2.6.1 *Si dice* variazione *della sequenza dei coefficienti di $p(x)$, ogni coppia di coefficienti consecutivi che abbiano segno opposto.*

Si può dimostrare la seguente proposizione, detta *regola dei segni di Cartesio*:

Proposizione 2.6.2 *Sia $p \in \mathbb{R}[x]$ un polinomio che abbia* tutte le radici reali*. Allora il numero di quelle positive è uguale al numero delle variazioni dei segni nella sequenza dei coefficienti di p.*

Esempio 2.6.3 *Consideriamo il polinomio $p(x) = x^4 - 6x^3 + 9x^2 - 3x$. Supponiamo di sapere che esso ha tutte le radici reali. La sequenza dei coefficienti di p è data da $+1, -6, +9, -3$. Vi sono tre variazioni, $(1, -6)$, $(-6, 9)$ e $(9, -3)$. Dunque p ha tre radici positive.*

2.7 Esercizi

1) Scomporre in fattori lineari (a coefficienti reali o complessi) i seguenti polinomi:

$$x^3 - 6x^2 + 11x - 6\,,$$
$$x^4 + 4\,,$$
$$x^4 + 4x^3 + 4x^2 + 1\,,$$
$$x^4 - 10x^2 + 1\,.$$

2) Scomporre in fattori reali irriducibili i seguenti polinomi:

$$x^2 + 4\,,$$
$$x^6 + 27\,,$$
$$x^4 + 4x^3 + 4x^2 + 1\,.$$

Capitolo 3

MATRICI

3.1 Matrici

Una tabella di numeri reali (o complessi) o di elementi di un qualunque insieme numerico) ordinati su m righe orizzontali e n colonne verticali si chiama *matrice* a valori reali (risp. complessi o quello che sia) di *tipo* $m \times n$.

Ad esempio:

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 \\ -1 & \sqrt{2} & 1 & 0 \\ \frac{1}{3} & -2 & 3 & 1 \end{pmatrix}$$

è una matrice a valori reali di tipo 3×4.

Osserviamo che ogni elemento della matrice A è individuato da una coppia di indici i, j interi positivi, nel modo che l'elemento a_{ij} di A è quello che si trova all'incrocio tra la i-esima riga e la j-esima colonna. Si usa scrivere (a_{ij}) per indicare la matrice (di tipo opportuno) i cui elementi sono a_{ij}.

Nel nostro esempio, $a_{32} = -2$, mentre $a_{14} = 0$.

Se $m = n$, cioè la matrice data ha tante righe quante colonne, tale matrice viene detta matrice *quadrata* e il numero n viene detto *ordine* della matrice. La matrice

$$B = \begin{pmatrix} \frac{1}{4} & -1 & 1 \\ -1 & \sqrt{3} & 1 \\ 0 & -4 & 7 \end{pmatrix}$$

è una matrice quadrata di ordine 3.

In una matrice quadrata, l'insieme dei valori a_{ii} che hanno l'indice di riga uguale all'indice di colonna viene detto *diagonale principale*.

Le matrici di tipo $n \times 1$ si chiamano anche, per ovvio impatto visivo, *colonne*, mentre le matrici di tipo $1 \times m$ si chiamano *righe*.

L'insieme delle matrici a valori reali di tipo $m \times n$ si indica con $\mathbf{M}_{m,n}(\mathbb{R})$ mentre l'insieme delle matrici quadrate di ordine n si indica con $\mathbf{M}_n(\mathbb{R})$. Una notazione analoga si usa per le matrice a valori complessi.

3.2 Operazioni tra matrici

Sulle matrici dello stesso tipo, cioè sull'insieme $\mathbf{M}_{m,n}(\mathbb{R})$, è possibile definire la seguente operazione di *somma*.

Definizione 3.2.1 *Date $A, B \in \mathbf{M}_{m,n}(\mathbb{R})$, $A = (a_{ij})$ e $B = (b_{ij})$, la loro somma $A+B$ è la matrice $C \in \mathbf{M}_{m,n}(\mathbb{R})$ che ha come elemento c_{ij} la somma dei corrispondenti elementi di A e B:*

$$c_{ij} = a_{ij} + b_{ij} \qquad \text{dove } i = 1\ldots, m \text{ e } j = 1, \ldots, n\,.$$

Esempio 3.2.2

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \; B = \begin{pmatrix} -2 & 0 & -1 \\ 1 & -1 & \frac{1}{2} \end{pmatrix}, \; C = A + B = \begin{pmatrix} -1 & 1 & 0 \\ 2 & -2 & \frac{1}{2} \end{pmatrix}.$$

Proposizione 3.2.3 *L'insieme $\mathbf{M}_{m,n}(\mathbb{R})$ munito della operazione di somma così definita è un gruppo abeliano.*

Dim. Ci limitiamo ad osservare che l'associatività e la commutatività di questa operazione derivano immediatamente dalle analoghe proprietà della somma tra numeri reali. Segnaliamo che, se 0 indica la matrice che ha tutti i suoi termini uguali a zero, essa è l'elemento neutro della somma tra matrici, mentre l'opposta di A, indicata con $-A$, è la matrice che ha in ogni posto il valore di A cambiato di segno. □

Definizione 3.2.4 *Se $A \in \mathbf{M}_{n,m}(\mathbb{R})$ e $\lambda \in \mathbb{R}$, il* prodotto di A per lo scalare λ *è la matrice che ha al posto i, j l'elemento λa_{ij} dove a_{ij} è il valore di A al posto corrispondente.*

Esempio 3.2.5

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix}, \quad \frac{1}{2}A = \begin{pmatrix} \frac{1}{2} & 1 \\ 0 & -\frac{3}{2} \end{pmatrix}.$$

Osserviamo che

$$(-1)A = -A \quad \text{e} \quad 0A = 0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}.$$

In alcuni casi è utile poter costruire una matrice partendo da certe altre matrici tutte dello stesso tipo, utilizzando le due operazioni sopra definite di somma e di prodotto per scalare.

Definizione 3.2.6 *Una matrice A si dice* combinazione lineare *delle matrici $A_1, \dots, A_n$, tutte dello stesso tipo, se risulta:*

$$A = \lambda_1 A_1 + \cdots + \lambda_n A_n$$

per opportuni coefficienti $\lambda_i \in \mathbb{R}$.

Definizione 3.2.7 *Il* prodotto riga per colonna *di una matrici A di tipo $n \times m$ e di una matrice B di tipo $m \times p$ è l'operazione che associa alla coppia ordinata (A, B) la matrice C di tipo $n \times p$ nel seguente modo:*

$$c_{ij} = a_{i1}b_{1j} + \ldots + a_{im}b_{mj}\,.$$

In altri termini, l'elemento c_{ij} di C si ottiene prendendo la i-esima riga di A e la j-esima colonna di B; poi moltiplicando il primo elemento della riga con il primo elemento della colonna, il secondo con il secondo e così via fino allo m-esimo (e ultimo); infine si sommano tutti questi m prodotti.
Indichiamo la matrice prodotto C con $A \cdot B$ o semplicemente AB.

Da notare che per questa definizione è essenziale che il numero di elementi che compongono una riga di A (cioè il numero delle sue colonne) sia uguale al numero di elementi che compongono una colonna di B (cioè il numero delle sue righe). Il risultato è una matrice che lo stesso numero di righe di A e lo stesso numero di colonne di B.

Esempio 3.2.8

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 0 \\ 1 & -1 & 0 \\ -1 & 3 & 0 \end{pmatrix},$$

$$\begin{array}{lll} c_{11} = 1 + 1 - 1 = 1\,, & c_{12} = 2 - 1 + 3 = 4\,, & c_{13} = 0 + 0 + 0 = 0\,, \\ c_{21} = 1 - 1 + 0 = 0\,, & c_{22} = 2 + 1 + 0 = 3\,, & c_{23} = 0 + 0 + 0 = 0\,, \end{array}$$

$$C = A \cdot B = \begin{pmatrix} 1 & 4 & 0 \\ 0 & 3 & 0 \end{pmatrix}.$$

Proposizione 3.2.9 *Il prodotto riga per colonna tra matrici gode delle seguenti proprietà:*

1. *È associativo. Ciò significa che* $(A \cdot B) \cdot C = A \cdot (B \cdot C) = A \cdot B \cdot C$.
2. *È distributivo sia a destra che a sinistra rispetto alla somma. Cioè*
$$(A + B) \cdot C = A \cdot C + B \cdot C \quad \text{e} \quad M \cdot (N + P) = M \cdot N + M \cdot P\,.$$
3. *La matrice* I_n *di tipo* $n \times n$ *tale che*
$$i_{ij} = \begin{cases} 0 & se\ i \neq j\,, \\ 1 & se\ i = j\,, \end{cases}$$
cioè la matrice quadrata con tutti 1 *sulla diagonale principale e* 0 *altrove, è tale che* $A \cdot I_n = A$ *e* $I_n \cdot B = B$ *per tutte le matrici* A *e* B *per cui il prodotto risulta definito.*

In particolare, $\mathbf{M}_n(\mathbb{R})$ *è un anello con identità (si dice anche unitario), essendo* I_n *l'elemento neutro del prodotto.*

La dimostrazione di queste proprietà viene lasciata per esercizio, per la verità nemmeno molto utile. È però importante osservare che il prodotto riga per colonna *non* gode della proprietà commutativa. In molti casi addirittura A e B sono tali che pur essendo definito il prodotto $A \cdot B$, risulta che $B \cdot A$ non si può nemmeno calcolare. Basta pensare all'esempio precedente dove, essendo A di tipo 2×3 e B di tipo 3×3, il prodotto $B \cdot A$ non è definito. Ma anche nel caso in cui fossero definiti entrambi $A \cdot B$ e $B \cdot A$, come accade per la matrici quadrate dello stesso ordine, in generale si ha che $AB \neq BA$.

Esempio 3.2.10

$$A = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1}{3} \end{pmatrix}, \quad AB = \begin{pmatrix} 1 & \frac{2}{3} \\ \frac{1}{2} & \frac{1}{6} \end{pmatrix} \neq BA = \begin{pmatrix} 2 & -\frac{3}{2} \\ 1 & -\frac{5}{6} \end{pmatrix}.$$

Un altro tabù del calcolo elementare è violato dal prodotto riga per colonna: può accadere che A e B siano matrici non nulle, ma $A \cdot B = 0$.

Esempio 3.2.11

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Introduciamo ora la trasposizione di matrici.

Definizione 3.2.12 *Data una matrice A di tipo $n \times m$, la matrice $B = (b_{ij})$ di tipo $m \times n$ tale che $b_{ij} = a_{ji}$ si dice matrice* trasposta *di A e si indica con ${}^tA$.*

In altre parole $B = {}^tA$ è la matrice di tipo $m \times n$ che ha come i-esima riga la i-esima colonna di A.

Esempio 3.2.13

$$A = \begin{pmatrix} 1 & 3 & \sqrt{2} & 0 \\ -1 & \frac{1}{2} & \frac{1}{3} & \frac{2}{3} \\ 0 & -1 & 4 & 2 \end{pmatrix}, \quad {}^tA = \begin{pmatrix} 1 & -1 & 0 \\ 3 & \frac{1}{2} & -1 \\ \sqrt{2} & \frac{1}{3} & 4 \\ 0 & \frac{2}{3} & 2 \end{pmatrix}.$$

È facile verificare che ${}^t(A + B) = {}^tA + {}^tB$. Invece, per ciò che concerne il prodotto riga per colonna, vale la seguente regola:

$$ {}^t(AB) = {}^tB\,{}^tA\,, \tag{3.1}$$

cioè la trasposizione inverte l'ordine dei fattori e, poiché il prodotto non è commutativo, il fatto riveste una certa importanza.

Dimostriamolo brevemente. Se $C = {}^t(AB)$, c_{ij} è l'elemento al posto j, i di $A \cdot B$. Questo si ottiene moltiplicando la j-esima riga di A con la i-esima colonna di B. Se $D = {}^tB\,{}^tA$, allora d_{ij} si ottiene moltiplicando la i-esima riga di ${}^tB$ per la j-esima colonna di ${}^tA$. Ma poiché la la j-esima riga di A coincide con la j-esima colonna di ${}^tA$ e la i-esima riga di ${}^tB$ coincide con la i-esima colonna di B, $c_{ij} = d_{ij}$ e quindi $C = D$.

3.3 Matrici quadrate

Introduciamo ora dei tipi di matrici quadrate di particolare interesse.

3.3.1 Matrici simmetriche e antisimmetriche

Definizione 3.3.1 *Una matrice A (quadrata) si dice* simmetrica *se $A = {}^tA$.*

Esempio 3.3.2

$$A = \begin{pmatrix} -1 & 3 & 0 \\ 3 & 11 & 2 \\ 0 & 2 & \frac{1}{2} \end{pmatrix} = {}^tA\,.$$

Definizione 3.3.3 *Una matrice A (quadrata) si dice* antisimmetrica *se $A = -\,{}^tA$.*

Esempio 3.3.4

$$A = \begin{pmatrix} 0 & 2 & -1 & \frac{1}{2} \\ -2 & 0 & 7 & -\frac{2}{3} \\ 1 & -7 & 0 & 1 \\ -\frac{1}{2} & \frac{2}{3} & -1 & 0 \end{pmatrix} = -\,{}^tA\,.$$

Da osservare che una matrice antisimmetrica ha sempre tutti 0 sulla diagonale principale perché, dovendo essere $a_{ii} = -a_{ii}$, si ha che $a_{ii} = 0$.

Osservazione 3.3.5 *Se A è una matrice quadrata, allora $A + {}^tA$ è simmetrica e $A - {}^tA$ antisimmetrica. Se A è una matrice a coefficienti reali (si dice brevemente "reale"), allora A è somma di una matrice simmetrica e una antisimmetrica, come segue subito dall'uguaglianza*

$$A = \frac{1}{2}(A + {}^tA) + \frac{1}{2}(A - {}^tA)\,.$$

Si può dimostrare che tale scrittura è anche unica, cioè, se A' e A'' sono due matrici, la prima simmetrica e la seconda antisimmetrica, tali che $A = A' + A''$, allora necessariamente $A' = \frac{1}{2}(A + {}^tA)$ e $A'' = \frac{1}{2}(A + {}^tA)$.

3.3.2 Matrici triangolari

Definizione 3.3.6 *Una matrice quadrata A si dice* triangolare *(superiore) se tutti i suoi elementi posti sotto la diagonale principale sono nulli. Ossia:*

$$a_{ij} = 0 \text{ se } i > j\,.$$

In modo analogo si definiscono le matrici triangolari inferiori.

Esempio 3.3.7

$$A = \begin{pmatrix} 1 & 2 & 2 & 1 \\ 0 & 1 & 3 & 2 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Osservazione 3.3.8 *La somma e il prodotto riga per colonna tra matrici triangolari danno come risultato una matrice triangolare.*

Questo fatto è ovvio per la somma. Per quanto riguarda il prodotto $C = A \cdot B$, $c_{ij} = a_{i1}b_{1j} + \cdots + a_{in}b_{nj}$, dove A e B sono triangolari, abbiamo quanto segue.

Se $i > j$, per $1 \leq k \leq j$, sicuramente $a_{ik} = 0$, mentre per $j < k \leq n$ sicuramente $b_{kj} = 0$.

Quindi tutti i termini che esprimono c_{ij} per $i > j$ sono nulli e pertanto, $c_{ij} = 0$, per $i > j$.

Non solo. L'i-esimo elemento sulla diagonale principale di C è uguale al prodotto degli i-esimi elementi delle diagonali principali di A e B rispettivamente: $c_{ii} = a_{ii}b_{ii}$.

3.4 Trasformazioni elementari di riga

Definizione 3.4.1 *Si dice* trasformazione (o operazione) elementare di riga di primo tipo *l'operazione che associa alla matrice A di tipo $m \times n$ (quindi anche non quadrata) una matrice A' (dello stesso tipo di A) che si ottiene da A scambiando tra loro di posto due righe di A.*

Definizione 3.4.2 *Si dice* trasformazione (o operazione) elementare di riga di secondo tipo *l'operazione che associa alla matrice A di tipo $m \times n$, una matrice A' (dello stesso tipo di A) che si ottiene da A sommando ad una riga di A una combinazione lineare delle altre righe di A.*

Definizione 3.4.3 *Si dice* trasformazione (o operazione) elementare di riga di terzo tipo *l'operazione che associa alla matrice A di tipo $m \times n$, una matrice A' (dello stesso tipo di A) che si ottiene da A moltiplicando una riga di A per uno scalare λ* non nullo.

Con analoghe definizioni si possono introdurre le operazioni elementari di colonna, per cui varranno proprietà analoghe.

Introduciamo per comodità le matrici $E_{i,j}$, di tipo $m \times n$ opportuno (eventualmente quadrate), che hanno 1 come elemento di posto i, j e 0 altrimenti. Allora abbiamo:

Osservazione 3.4.4 *1) Dati i, j, interi positivi, si consideri la matrice quadrata di ordine n:*

$$T' = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}\,. \tag{3.2}$$

Si provi a scrivere esplicitamente una tale matrice. Abbiamo che, se A è una qualsiasi matrice $n \times m$, allora $T' \cdot A$ è la matrice che si ottiene da A scambiando fra loro la riga di posto i con quella di posto j.

2) Dati dei coefficienti $\lambda_1, \ldots, \lambda_{i-1}, \lambda_{i+1}, \ldots, \lambda_n$, sia

$$\begin{aligned} T'' &= I_n + \lambda_1 E_{i,1} + \cdots + \lambda_{i-1} E_{i,i-1} + \lambda_{i,i+1} E_{i,i+1} + \cdots + \lambda_n E_{i,n} \qquad (3.3) \\ &= \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \lambda_1 & \cdots & \lambda_{i-1} & 1 & \lambda_{i+1} & \cdots & \lambda_n \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \end{aligned}$$

dove, con una convenzione che spesso useremo, gli elementi della matrice non indicati sono considerati nulli.

La matrice $T'' \cdot A$ è allora la matrice che si ottiene da A sommando alla riga i-esima una combinazione lineare delle altre (con coefficienti λ_k).

3) Dato uno scalare λ, sia infine

$$\begin{aligned} T''' &= I_n + (\lambda - 1)E_{i,i} \\ &= \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}. \end{aligned} \tag{3.4}$$

In questo caso la matrice $T''' \cdot A$ si ottiene da A moltiplicando la sua riga i-esima per λ.

Definizione 3.4.5 *Due matrici A e B si dicono* equivalenti per operazioni di riga *se una può essere ottenuta dall'altra mediante l'applicazione successiva di trasformazioni elementari di riga dei vari tipi. Scriveremo che $B = T_R(A)$.*

Analogamente si può introdurre l'equivalenza per operazioni di colonna. Scriveremo che $B = T_C(A)$.

Osservazione 3.4.6 *Se B è una matrice equivalente a A, cioè $B = T_R(A)$, allora $B = T \cdot A$, con T prodotto di matrici del tipo mostrato in (3.2),(3.3) e (3.4).*

Proposizione 3.4.7 *Con le notazioni sopra, valgono le seguenti formule:*

1) $T_R(A) \cdot B = T_R(A \cdot B)$;

2) $A \cdot T_C(B) = T_C(A \cdot B)$.

Dim. Per l'Osservazione 3.4.6, usando la proprietà associativa del prodotto righe per colonne, si ha subito

$$T_R(A) \cdot B = (T \cdot A) \cdot B = T \cdot (A \cdot B) = T_R(A \cdot B)\,.$$

Analogamente si dimostra la seconda formula. □

La seguente proposizione e il procedimento usato nella sua dimostrazione saranno di fondamentale importanza per quanto segue, in particolare per la risoluzione dei sistemi lineari.

Proposizione 3.4.8 *Ogni matrice quadrata A è equivalente per righe (per colonne) ad una matrice triangolare A'.*

La matrice A' può essere ottenuta da A usando solo trasformazioni del secondo *tipo.*

Dim. Dimostriamolo per induzione sull'ordine n della matrice A. Se $n = 1$, ogni matrice è triangolare.

Sia A una matrice quadrata di ordine n. Se tutta la prima colonna di A è fatta di zeri, allora applicando l'ipotesi induttiva alla matrice A_{11}, cioè la matrice di ordine $n - 1$ ottenuta cancellando da A la prima riga e la prima colonna, questa sarebbe equivalente ad una matrice triangolare tramite una successione di trasformazioni di riga. Ma applicando le stesse trasformazioni elementari ad A, poiché esse lasciano immutati i termini della prima colonna, essendo questi tutti zero, si otterrà una matrice triangolare. Se invece la prima colonna di A non è tutta di zeri, possiamo supporre che sia $a_{11} \neq 0$. Se così non fosse, sia $a_{i1} \neq 0$. Allora si sommi alla prima riga la i-esima. Adesso la matrice così ottenuta ha il termine di posto $1, 1$ non nullo. Per ogni $i = 2, \ldots, n$, si sommi alla i-esima riga, la prima riga moltiplicata per $\mu_i = -\frac{a_{i1}}{a_{11}}$, dove, appunto, a_{i1} è il primo termine della i-esima riga. Ora la nuova i-esima riga così ottenuta avrà come primo termine 0. Alla fine, tutta la prima colonna della matrice equivalente ad A avrà la prima colonna tutta di zeri, escluso al più il primo termine. Applicando l'ipotesi induttiva a A_{11}, come spiegato prima, o alternativamente, ripetendo questo stesso procedimento su A_{11}, che lascia invariata la prima colonna di A, si ha la tesi.

Analogo procedimento per le trasformazioni elementari sulle colonne, per le quali il procedimento parte dall'ultima riga (anziché dalla prima colonna).

$\square$

3.5 Determinanti

Sono state definite varie funzioni sull'insieme delle matrici *quadrate* che fossero particolarmente significative. Tra queste sicuramente la più rilevante è la funzione *determinante*. Tra le proprietà più importanti del determinante